IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation	)	Case No. 1:21-cv-00135
	)	Hon. Sharon Johnson Coleman

CLEARVIEW DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

Plaintiffs ask the Court to do something that no court appears to have ever done before—issue a preliminary injunction under the Illinois Biometric Information Privacy Act ("BIPA"). Plaintiffs make their unprecedented request based on *no* evidence of a BIPA violation or imminent harm to the putative class. They submit not a single affidavit or declaration in support, and offer nothing more than citations to newspaper articles in support of their claims. That alone is sufficient reason to deny Plaintiffs' motion, which requires them to come forward with evidence in support of their claims. Instead of providing evidence, Plaintiffs focus on their own, unsubstantiated and speculative opinions of the "dangers" of Clearview's product, while ignoring the substantial, concrete harm that Clearview and the public would experience if an injunction issued. Plaintiffs' speculation does not warrant a grant of the "extraordinary and drastic remedy" of a preliminary injunction. *Goodman v. Ill. Dep't of Fin. & Prof'l Regulation*, 430 F.3d 432, 437 (7th Cir. 2005). Because it fails to satisfy every element necessary for an injunction to issue, Plaintiffs' motion should be denied.

As a threshold matter, Plaintiffs have failed to show that Clearview's current operations violate BIPA. And Defendants have submitted substantial evidence—in the form of sworn affidavits and declarations—that demonstrates that Clearview does not because, among other things, it operates solely as an agent or subcontractor of governments and government agencies. *See* 740 ILCS 14/25(e). Plaintiffs ground their motion on the demonstrably false and entirely unsupported suggestion that the record evidence is untrue or cannot be trusted. However, because the uncontroverted record evidence establishes that Clearview operates within an exemption to BIPA, Plaintiffs cannot show (1) a likelihood of success on the merits, (2) irreparable harm, or (3) that the balance of equities favors an injunction.

As to the likelihood of success, Plaintiffs fail to address *any* of the following defenses, which Clearview will litigate here: applying BIPA to Clearview would violate the extraterritoriality doctrine of Illinois and the dormant Commerce Clause of the U.S. Constitution; applying BIPA here would violate the First Amendment to the U.S. Constitution; and BIPA does not apply here because Clearview uses its facial recognition app solely as an agent or contractor of government agencies. By failing to address any of these defenses, Plaintiffs cannot demonstrate on this record that they have a likelihood of success on the merits.

And without a violation of BIPA, Plaintiffs cannot demonstrate *any* harm, let alone irreparable harm.[1] Moreover, Clearview represents to this Court that it will inform the Court and Plaintffs if, during the pendency of this litigation, Clearview changes its current practice of serving solely as an agent or subcontractor of governments and government agencies. Declaration of Thomas Mulcaire ("Mulcaire Decl.") ¶ 49. Accordingly, there is no current threat of irreparable harm resulting from any of Clearview's future, speculative conduct.

Finally, Plaintiffs have failed to demonstrate that the balance of equities favors an injunction. Given that Clearview currently operates solely as an agent or subcontractor of governments and government agencies, Plaintiffs can point to no harm absent an injunction. In contrast, Clearview would be significantly harmed by an injunction because, depending on the relief fashioned, an injunction could force Clearview to cease operations nationwide. Moreover, the injunction requested would infringe Clearview's First Amendment rights. The public interest would also suffer if an injunction were entered, since government agencies would no longer be able to use Clearview's technology—a use that is expressly permitted under BIPA and that the

[1] Even if there were a violation of BIPA, Plaintiffs have failed to demonstrate that they lack an adequate remedy at law absent injunctive relief, given that BIPA provides for statutory damages.

declarations and affidavits submitted in support of this motion clearly establish would negatively impact the public's interest in effective law enforcement.

For those reasons, and those that follow, Plaintiffs' motion should be denied.

BACKGROUND

A. Clearview's Product and Operations

Clearview collects publicly-available images on the Internet and organizes them into a searchable database, which Clearview's licensed users can then search by using Clearview's app. Consolidated Class Action Complaint, dkt. 29 ("Compl.") ¶ 29; Mulcaire Decl. ¶ 7. Clearview's app is a tool used by government agencies to help solve crimes. Mulcaire Decl. ¶¶ 17-19; Affidavit of Kevin Metcalf ("Metcalf Aff.") ¶ 19; Affidavit of Jason Webb ("Webb Aff.") ¶ 17; Affidavit of Michael Williams ("Williams Aff.") ¶ 17. Clearview does not market, license, or sell any other products. Mulcaire Decl. ¶ 12.

Clearview collects images for its search engine without knowing the identities of the people depicted in the images. *Id.* ¶ 9. The only information that Clearview stores from the photos are: (1) the URL from which the photo was collected; (2) any metadata associated with the image itself; and (3) the facial vectors from the faces that appear in the image. *Id.* ¶ 10. Accordingly, Clearview cannot determine whether the individuals in the images it collects live in Illinois. *Id.* ¶ 9. At best, Clearview can tell—in some instances—where a photo was taken based on its available metadata. *Id.* Because Clearview cannot determine which individuals depicted in the photographs in its database reside in Illinois, if Clearview were ordered to remove all images of Illinois residents from its database, it could not do so. *Id.* ¶ 11. To comply with such an order, Clearview would likely have to cease using its database altogether, which would shut down its operations nationwide—even in states that permit Clearview's activities. *Id.*

Under no circumstances does Clearview sell, lease, trade, disseminate, disclose, or provide access to any facial vectors to its customers. *Id.* ¶ 15. Access to Clearview's database of facial vectors is restricted to a small number of employees with the highest administrative access at Clearview. *Id.* ¶ 30. The only information Clearview provides to users of its app is photographs and links to the websites containing those photographs. *Id.* ¶ 14.

Clearview has *never* experienced a data security incident or hack related to its collection of facial vectors or even its database of photos. *Id.* ¶ 27. Clearview has implemented reasonable safeguards to secure that data, including (i) a credentialing program to confirm that any licensee of the Clearview app, including a holder of a free-trial license, is who the licensee purports to be; (ii) a system to ensure that any new users of the Clearview app are authorized by their employers to use the app; (iii) dual-factor authentication such that by default, every log-in session is tied to a proven email address; (iv) encryption of the facial vectors generated by Clearview; (v) the implementation of a bug-bounty program; (vi) the deployment of anti-intrusion devices, such as firewalls and virus scanners; (vii) background checks of employees and contractors; (viii) employee cybersecurity training; (ix) requirements that employees use only electronic devices issued by Clearview for official tasks, and that these devices be accessible to Clearview's information-technology function, which monitors the devices for security threats; (x) engaging a third-party audit of the application's code by a cyber-security and risk management firm to identify and close vulnerabilities; and (xi) blocking access to Clearview's application by IP addresses in numerous countries, including high-risk countries. *Id.* ¶ 26.

Clearview's website has a policy detailing its retention schedule and guidelines for permanently destroying information that might be governed by BIPA. *Id.* ¶ 25 & Exh. C.

B. Clearview's Voluntary Changes to Its Business

Clearview has voluntarily changed its business practices over the past year. Clearview cancelled the accounts of every customer who was not either associated with government agencies or their agents or subcontractors. *Id.* ¶ 34. All photos in Clearview's database that have metadata associating them with a geolocation in Illinois are blocked from being searched through Clearview's app. *Id.* ¶ 36. Clearview constructed a "geofence" around Illinois, and stopped collecting facial vectors from images that contain metadata associating them with Illinois. *Id.* ¶ 40. Although Clearview cannot exclude with certainty every Illinois resident from its database, Clearview has taken reasonable steps to avoid collecting such images, even if these steps are over-inclusive and will exclude photos of many non-Illinois residents. *Id.* ¶ 41.

Clearview also implemented an opt-out mechanism for Illinois residents to exclude their photos from Clearview's search engine. *Id.* ¶ 42 & Exh. D. To exclude photographs from future inclusion in the Clearview search engine, Clearview, by necessity, must obtain a photograph of the individual who wishes to be excluded and create a facial vector that can then be used to ensure that the person's image is neither collected in the Clearview database nor included in search results on the Clearview app. *Id.* ¶ 43. Because Clearview's app searches only for facial vectors, and stores no other personal information about an individual in a photo, without this information, there would be no way to allow an individual to "opt-out" of Clearview's database and from search results on the Clearview app. *Id.* For this reason, Clearview's opt-out system requires that the person opting out consent to the creation of a facial vector that will be used solely for purposes of excluding them from the Clearview app. *Id.* ¶ 44. Thus, far from "tricking Illinois residents into consenting to the harvesting of their Biometric Data," Br. at 13, Clearview informs Illinois residents that it needs and uses their information solely for the opt-out system. Moreover, any facial vectors created for opt-out purposes are subject to strict controls and are used solely for

purposes of excluding the individual from the Clearview database and Clearview search results. Mulcaire Decl. ¶ 45.

Finally, Clearview's terms of use require users of the Clearview app to, among other things, agree to use the app only for law enforcement purposes and not to upload photos of Illinois residents. *Id.* ¶¶ 23, 38. Every customer that uses the Clearview app must also agree to "expressly authorize Clearview AI to act as an agent on [their] behalf for the purpose of (i) collecting and compiling publicly available images from the Internet and (ii) producing facial vectors from those images for the purpose of providing the Service to [them]." *Id.* ¶ 21 & Exh. B.

C. Clearview's Continued Commitment to Its Business Changes

Clearview informed this Court about these changes to its business practices in May 2020. *Mutnick v. Clearview*, 20-cv-512, ECF No. 56-2 ¶¶ 15-25. Plaintiffs assert that Clearview "cannot be trusted" to maintain these changes. Br. at 1. Yet, Clearview continues to operate as it told the Court it would a year ago, Mulcaire Decl. ¶ 46, and Plaintiffs do not suggest otherwise. Clearview represents to the Court it "will inform the Court and Plaintiffs if, at any point during the pendency of this litigation, Clearview decides to offer products or services to customers who are not law-enforcement agencies or governmental entities or their agents." *Id.* ¶ 49.

Finally, Plaintiffs argue that Clearview's 2020 patent application "describes a much broader use of [Clearview's] technology," Br. at 8, but this statement is grossly misleading.[2] A consent-based app on an individual's mobile phone that uses facial recognition would be fully

[2] As Clearview has explained to Plaintiffs, Clearview applied for a patent in August 2019—before it made the business changes detailed above. Mulcaire Decl. ¶ 48. On August 7, 2020, Clearview filed a formal application with the patent office that *required* Clearview to use the same description as the initial application to preserve its intellectual property. *Id.*; *see Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997) ("the specification [in a prior application] must contain an equivalent description of the claimed subject matter."). That the 2020 description matched an old description—because of a requirement of patent law—does not change Clearview's commitment to its business changes.

lawful and would be similar to existing uses by other technology companies. However, whatever the patent application says, at this time, Clearview does not intend to make its facial recognition app available to anyone other than governmental entities or their agents or subcontractors. Mulcaire Decl. ¶ 48.

LEGAL STANDARD

"[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, *by a clear showing*, carries the burden of persuasion." *Goodman v. Ill. Dep't of Fin. & Prof'l Regulation*, 430 F.3d 432, 437 (7th Cir. 2005) (quoting *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997)); *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) (the "requirement for substantial proof" on a preliminary injunction is "much higher" than that on summary judgment). To justify this relief, Plaintiffs have the burden of showing that: "(1) they have a reasonable likelihood of success on the merits; (2) no adequate remedy at law exists; (3) they will suffer irreparable harm, which, absent injunctive relief, outweighs the irreparable harm [Clearview] will suffer if the injunction is granted; and (4) the requested injunction will not harm the public interest." *Goodman*, 430 F.3d at 437. "[I]f [Plaintiffs] cannot satisfy any one of these threshold showings, the court's inquiry ends, and a preliminary injunction will not be issued." *Piekosz-Murphy v. Bd. of Educ. of Cmty. High Sch. Dist. No. 230*, 858 F. Supp. 2d 952, 961 (N.D. Ill. 2012). Clearview has been unable to find *any* reported case in which a plaintiff suing under BIPA has met this burden, and there is no reason to make this case the first one.

Rather than litigate the issue of a preliminary injunction based on facts and evidence, Plaintiffs have turned to attacks on the credibility of Clearview and its general counsel. Br. at 9. For reasons that Clearview has previously explained to the Court, those attacks are unfounded. *See Mutnick v. Clearview*, 20-cv-512, ECF No. 65. If, however, the Court has any reason to doubt the credibility of Clearview or its witnesses, the appropriate next step should be an evidentiary

hearing, *not* the imposition of a company-threatening injunction. *See Ty, Inc. v. GMA Accessories, Inc.*, 132 F.3d 1167, 1171 (7th Cir. 1997) ("If genuine issues of material fact are created by the response to a motion for a preliminary injunction, an evidentiary hearing is indeed required."); *Medeco Sec. Locks, Inc. v. Swiderek*, 680 F.2d 37, 38 (7th Cir. 1981) ("It is well established that, in general, a motion for a preliminary injunction should not be resolved on the basis of affidavits alone. Normally, an evidentiary hearing is required to decide credibility issues.").

ARGUMENT

I. Clearview's Operations Are Exempt From BIPA

Most importantly, Plaintiffs' requested injunction must be rejected because the record evidence establishes that Clearview's current operations are exempt from BIPA because BIPA does not apply to "a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." 740 ILCS 14/25(e). Today, Clearview's only licensed users are government agencies or their contractors or agents, and each user must agree to appoint Clearview as its agent "for the purpose of (i) collecting and compiling publicly available images from the Internet and (ii) producing facial vectors from those images for the purpose of providing the Service to [the user]." Mulcaire Decl. ¶ 21. Because Clearview is exempt from BIPA, Plaintiffs cannot show (1) a likelihood of success on the merits, (2) irreparable harm, or (3) that the balance of equities favors an injunction.

Plaintiffs offer no meaningful argument—or any evidence at all—in response. Plaintiffs first claim that Clearview's limitation of its user base to government agencies "cannot be verified," Br. at 7, but Plaintiffs have offered no evidence in response to Clearview's unrebutted testimony that Clearview's current users are governments or governmental agencies. Mulcaire Decl. ¶ 34. Plaintiffs also attempt to sidestep this BIPA exemption by describing their "serious concerns" about law enforcement agencies using Clearview's product. Br. at 7. But Plaintiffs should take

up their "concerns" with the Illinois legislature, rather than ask the Court to re-write or disregard the statute, which expressly permits such uses.

II. Plaintiffs Cannot Show a Likelihood of Success on the Merits

To obtain an injunction, Plaintiffs are "required to establish . . . that there [is] a reasonable or substantial likelihood that [they will] succeed on the merits." *Teamsters Loc. Unions Nos. 75 & 200 v. Barry Trucking, Inc.*, 176 F.3d 1004, 1011 (7th Cir. 1999). "As part of the preliminary-injunction analysis, a district court may consider a nonmovant's defenses in determining the movant's likelihood of success on the merits." *Cassell v. Snyders*, 458 F. Supp. 3d 981, 990 (N.D. Ill. 2020), *aff'd*, 990 F.3d 539 (7th Cir. 2021).

Without submitting *any* evidence beyond citing to public news stories, and without addressing *any* of Clearview's defenses, Plaintiffs assert that they have a "high likelihood" of success on their BIPA claims. Br. at 14. In fact, the record evidence plainly supports not only the applicability of BIPA's statutory exemption for governmental agents, but also Clearview's other defenses, as set forth below.

A. BIPA Cannot Be Applied to Regulate Out-Of-State Conduct

Plaintiffs' case fails on the merits because (1) BIPA does not apply to conduct outside of Illinois and (2) the application of BIPA to Clearview would violate the dormant Commerce Clause.

First, Illinois has a "long-standing rule of construction" that a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184-85, 835 N.E.2d 801, 852 (2005). Because BIPA expresses no such intent, courts in Illinois have repeatedly held that BIPA does not regulate out-of-state conduct. *See, e.g.*, *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1104 (N.D. Ill. 2017); *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017). The Illinois Supreme Court has explained that a "transaction may be said to

take place within a state if the circumstances relating to the transaction occur[red] *primarily and substantially*" in Illinois. *Avery*, 216 Ill. 2d at 186, 835 N.E.2d at 853 (emphasis added). To satisfy this standard, the "*majority* of circumstances relating to the alleged violation" of the statute must have occurred in Illinois. *Landau v. CNA Fin. Corp*, 381 Ill. App. 3d 61, 65, 886 N.E.2d 405, 409 (1st Dist. 2008) (emphasis added).

The record evidence, however, establishes that the "majority of circumstances" giving rise to Plaintiffs' claims occurred outside of Illinois. Specifically, Clearview operates from its headquarters in New York; Clearview's servers are located outside of Illinois; and Clearview does not sell its services or app to anyone in Illinois.[3] Mulclaire Decl. ¶¶ 2-5, 40. Thus, Plaintiffs' BIPA claim fails under Illinois's extraterritoriality doctrine.

Second, Plaintiffs' proposed application of BIPA to Clearview violates the dormant Commerce Clause of the U.S. Constitution, which "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989). Illinois courts have "t[aken] a broad[] view" of what constitutes an inconsistent legal regime for dormant Commerce Clause purposes. *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667 (7th Cir. 2010). Specifically, a party need not show "inconsistent *obligations*"; rather, "the *absence* of [a] . . . counterpart" law in another state shows that the other state "thinks [the conduct] shouldn't be restricted in the [same] way." *Id.* (emphasis added).

[3] Clearview's past contracts with Illinois entities do not constitute any of the circumstances giving rise to Plaintiffs' claim because contracts with government agencies are explicitly exempt from BIPA, and no Clearview contract with an Illinois entity involves the sale, collection, or disclosure of biometrics in violation of BIPA.

Here, New York has considered BIPA-style legislation multiple times in recent years, but has never enacted such legislation. *See* A1911, Assemb., Reg. Sess. (N.Y. 2019); S1203, Senate, Reg. Sess. (N.Y. 2019); A9793, Assemb., Reg. Sess. (N.Y. 2018); S8547, Senate, Reg. Sess. (N.Y. 2018). Because Illinois has no interest in regulating Clearview's alleged conduct in New York, and because New York has declined to adopt a statute regulating biometrics, the dormant Commerce Clause precludes application of BIPA to Clearview, as finding otherwise would "exalt the public policy" of Illinois over that of New York. *Midwest Title Loans*, 593 F.3d at 668.

Applying BIPA to Clearview's conduct in New York (and elsewhere) would subject Clearview to liability under an Illinois statute because some small percentage of Clearview's database of publicly-available photographs are alleged to contain images of Illinois residents. Compl. ¶ 29. Moreover, the record evidence establishes that Clearview cannot associate an image with a specific person's identity in any automated fashion, and it is therefore impossible for Clearview to determine where the subjects of the images reside. Mulclaire Decl. ¶ 9. Clearview thus cannot determine whether the individuals in the images it collects from the Internet live in Illinois. *Id.* And as a result, "if Clearview were ordered to remove all images of Illinois residents from its database, Clearview would not be able to do so. To comply with such an order, Clearview would likely have to cease using its database altogether," which "would effectively shut down Clearview's operations nationwide—even in states that permit Clearview's activities." *Id.* ¶ 11. An injunction in this case would therefore impose precisely the kind of burden on interstate commerce that the dormant Commerce Clause prohibits.

B. Plaintiffs' Claim Is Barred by the First Amendment

1. Clearview Is Engaged in Speech That Is Protected by the First Amendment

The United States Supreme Court has unambiguously determined that the "creation and dissemination of information are speech within the meaning of the First Amendment." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). That is what Clearview does.

In *Sorrell*, the Court struck down a Vermont statute which banned the sale of prescriber-identifying information to drug companies. *Id.* at 571. In striking down the statute, the Court rejected the arguments that the Vermont law did not regulate speech, but rather just regulated "access to information" or conduct. *Id.* at 568. "Facts, after all," held the Court, "are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs." *Id.* at 570. The same reasoning applies to BIPA's restrictions on the collection and use of "biometric information." As applied to Clearview, BIPA violates the First Amendment by inhibiting Clearview's ability to collect, analyze, and include public information in its product, and preventing dissemination of truthful information regarding the identity of individuals pictured in law enforcement-submitted images.

Moreover, once "truthful information [is] 'publicly revealed' or 'in the public domain,'" a court may not "constitutionally restrain its dissemination." *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 103 (1979). Courts have repeatedly held that there is no right to privacy in materials posted on the Internet. *See Nieman v. VersusLaw, Inc.*, 512 F. App'x 635 (7th Cir. 2013) (affirming dismissal on First Amendment grounds because claims were "based on the defendants' republication of documents contained in the public record, so they fall within and are barred by the First Amendment privilege."); *United States v. Khan*, No. 15-cr-286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) (holding "[t]here is no expectation of privacy in a public Facebook page"

because there is no expectation of privacy "'when a computer user disseminates information to the public through a website'"), *aff'd*, 937 F.3d 1042 (7th Cir. 2019).[4] A similar First Amendment privilege protects Clearview's republication of publicly-available photos published on the Internet.

2. BIPA Is a Content- and Speaker-Based Restriction Subject to Strict Scrutiny

BIPA is subject to strict scrutiny because it is a content-based statute that "target[s] speech based on its communicative content." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). Plaintiffs' objection to Clearview's service is that Clearview efficiently matches publicly-available photographs using modern technology. BIPA does this by targeting specific content—defined as "Biometric Information" and "Biometric Identifiers," 740 ILCS 14/10—and not others (*e.g.*, photographs), simply because that content allows for what the government believes is a too-efficient means of identifying individuals. The objection therefore is content-based and is presumptively unconstitutional. *Reed*, 576 U.S. at 163.

BIPA is also subject to strict scrutiny because it is a "speaker-based" restriction on speech. *Sorrell*, 564 U.S. at 570. In *Sorrell*, the Supreme Court made clear that any law that imposes burdens on speech that apply to some speakers but not others, triggers heightened judicial scrutiny. *Id.* That is precisely what BIPA does in expressly exempting from its requirements any "financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999" and any "contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." 740 ILCS 14/25(c), (e).

[4] *See also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users [of the Internet] would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."); *Doe I v. Yesner*, No. 3:19-CV-0136-HRH, 2019 WL 4196054 (D. Alaska Sept. 4, 2019) (the use of photographs posted on plaintiff's social media profile could not support privacy-based causes of action).

3. BIPA Is Subject to, and Cannot Survive, Strict Scrutiny

Because BIPA imposes content-based and speaker-based restrictions on Clearview's speech, it is subject to, and cannot meet, strict scrutiny. *First*, BIPA serves no compelling state interest with respect to already-published public information—and no compelling interest here where Clearview only uses that information as an agent of government agencies and law enforcement. The stated purpose of BIPA is to protect the privacy of Illinois citizens. *See, e.g.*, *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020) (BIPA's "regime is designed to protect consumers against the threat of irreparable privacy harms"). But an individual's right to control his or her biometric information under BIPA does not apply if that right is relinquished. *See United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016) (recognizing there is no expectation of privacy in information that has already been disclosed to third parties). *Second*, even if the statute arguably served a compelling interest in protecting the privacy of individuals who placed photographs of themselves in the public realm (and it does not), BIPA is not narrowly tailored to achieve that interest. As applied to Clearview, BIPA would require it to provide written notice before collecting "biometric information." But as a matter of repeatedly decided law, individuals who post their photographs on the Internet effectively consent to sharing their images embodied in their photographs with the public at large. *See, e.g.*, *id.* at 806 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[.]").[5]

[5] Moreover, BIPA is unconstitutionally overbroad because of Clearview's inability to determine the identity of the photographed individuals. *See* Mulcaire Decl. ¶ 8 ("Clearview cannot associate an image with a specific person's identity in any automated fashion, and it is therefore impossible for Clearview to determine where the subjects of the images reside."). By requiring consent from all such individuals BIPA all but bars—and certainly severely burdens—Clearview's right to use previously-published, publicly-displayed photographs. In doing so, BIPA "suppresses a large amount of speech" that is fully protected under the First Amendment, precisely what the overbreadth doctrine exists to protect against. *Reno v. ACLU*, 521 U.S. 844, 874 (1997).

C. Clearview's Operations Are Exempt From BIPA

Finally, Plaintiffs' request for injunctive relief fails on the merits because the record evidence establishes that Clearview is exempt from BIPA since Clearview's only licensed users are government agencies or their contractors or agents, and an agency relationship is expressly created when governmental agencies use Clearview's services. *See supra* Part I.

III. The Harms to Clearview and to the Public Weigh Against Entry of an Injunction

When considering whether to enter an injunction, courts "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008). The Court should deny Plaintiffs' motion because Plaintiffs will not be harmed absent an injunction, and because Clearview and the public would suffer irreparable harm if an injunction were entered.

A. Plaintiffs Will Not Be Irreparably Harmed Absent an Injunction

Plaintiffs cannot obtain a preliminary injunction unless they can demonstrate that they "will suffer irreparable harm in the interim—that is, harm that cannot be prevented or fully rectified by the final judgment after trial." *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 386 (7th Cir. 1984). Plaintiffs claim that Clearview's alleged ongoing BIPA violations and the risk of a data breach will cause Plaintiffs irreparable harm. Br. at 12-13. However, these risks are either non-existent or speculative.

Most importantly, Plaintiffs cannot demonstrate *any* harm, let alone irreparable harm, because Clearview's current operations are exempt from BIPA. Moreover, Clearview represents to this Court that if, during the pendency of this litigation, it were to change its current practice of working solely with law enforcement or government entities or their agents, it commits to letting this Court and Plaintiffs' counsel know before it does so. Mulcaire Decl. ¶ 49. Given that, there is no current threat of irreparable harm.

Plaintiffs argue that they need an injunction to protect them from potential security breaches at Clearview, Br. at 13, but this contention lacks any factual support. Plaintiffs assert with no factual support that Clearview has a "lax attitude with respect to security," and that as a result, Plaintiffs are subject "to the ongoing prospect of injury." *Id.* However, in the year plus of this litigation, Plaintiffs cannot point to a single injury that actually has occurred because of these purportedly "lax" security practices. Instead of citing to any Clearview data breach that exposed their personal information (because they cannot), Plaintiffs cite to a data breach that occurred at *another company*—Equifax, and describe incidents at Clearview that did not impact any personal information.[6] *Id*. at 12. Contrary to Plaintiffs' unsubstantiated allegations, Clearview has robust security measures in place, and, despite regular attempts by hackers to access Clearview's data, no facial images or vectors collected by Clearview have ever been compromised. Mulcaire Decl. ¶ 27.

Plaintiffs' vague assertions about a "lax attitude towards security" without any factual support through declarations or otherwise cannot support Plaintiffs' burden of demonstrating irreparable harm. *See Pac. Trellis Fruit, LLC v. Agricola Yaurilla, S.A.*, No. 16-cv-4160, 2016 WL 9226379, at *1 (C.D. Cal. Oct. 17, 2016) (requiring more than speculative irreparable harm); *Outdoor Lighting Perspectives Franchising, Inc. v. Stubbs*, No. 11-cv-2524, 2012 WL 12904016, at *2 (D.S.C. June 15, 2012) (same).

Finally, Plaintiffs fail to show irreparable harm because many aspects of their requested injunction would not require Clearview to change its behavior.[7] For example, Plaintiffs seek to

[6] Plaintiffs cite news articles reporting that Clearview's customer list and Clearview's "internal files, apps and source code" were exposed as a result of data breaches. Br. at 7-8. No facial images collected by Clearview, law enforcement search histories, or other personal information were accessed during these incidents, and the vulnerabilities that led to those incidents have been addressed. Mulcaire Decl. ¶¶ 27-29.

[7] In addition to the activities discussed above that Plaintiffs seek to enjoin, Plaintiffs also seek to require

enjoin Clearview from "[d]istributing, redistributing or disseminating" or "[s]elling, trading leasing or otherwise profiting from Illinois residents' Biometric Data." Br. at 2. However, Clearview does not do any of these things, and never has. Mulcaire Decl. ¶¶ 15-16. Clearview has repeatedly informed Plaintiffs and this Court through sworn statements that it does not sell or disseminate biometric data. *Mutnick v. Clearview*, 20-cv-512, ECF No. 46-2 ¶ 6; ECF No. 56-2 ¶ 10. Plaintiffs have cited no evidence to dispute this fact. Because Clearview does not sell or otherwise disseminate biometric data, Plaintiffs will not be harmed absent a court order enjoining those activities. *See, e.g.*, *Kessler v. Pass*, No. 18-cv-530, 2018 WL 5307821, at *1 (S.D. Ill. Oct. 26, 2018) (injunctions sought for conduct that defendants have already voluntarily provided "serve no purpose" and should not be granted); *White v. Rozum*, No. 06-cv-244, 2007 WL 218709, at *2 (W.D. Pa. Jan. 25, 2007) (same).

B. Clearview Will Be Irreparably Harmed If Plaintiffs' Requested Injunctive Relief Is Granted

Even if Plaintiffs could demonstrate any harm to them, that harm would not outweigh the irreparable harm—being put out of business—that Clearview would experience if an injunction issued. *See Maxim's Ltd. v. Badonsky*, 772 F.2d 388, 392 (7th Cir. 1985).

The first part of Plaintiffs' requested relief seeks to enjoin Clearview from "[c]ontinuing to possess, use and store" Illinois residents' biometrics and from "[c]ollecting, capturing or obtaining" Illinois residents' biometric data without first providing notice and obtaining consent. Br. at 1-2. However, Plaintiffs' demand that Clearview stop collecting and using Illinois residents' facial vectors, even when doing so as an agent of governments and government agencies, is

---

Clearview to "[s]tore, transmit and protect from disclosure all Biometric Data of Illinois residents" and to "[d]evelop and publish on Defendant Clearview's website a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying Illinois residents' Biometric Data." Br. at 2. Clearview already protects from disclosure all personal data and already has a retention schedule on its website. Mulcaire Decl. ¶¶ 25-26.

improper because BIPA does not apply to agents of governments and government agencies. *See Air Serv Corp. v. Serv. Emps. Int'l Union, Loc. 1*, 225 F. Supp. 3d 745, 751 (N.D. Ill. 2016).

Even if Plaintiffs' requested relief did not conflict with BIPA, it would be impossible to implement without terminating Clearview's business in other states. Plaintiffs' claim that "[a]n injunction will not impact Defendants' ability to utilize the Biometric Database in 49 other states" is plainly wrong. Br. at 15. Because Clearview has no way of knowing which images on the public Internet are of Illinois residents, and which are of residents of other states, Clearview cannot simply stop collecting and using photos of Illinois residents unless it stops collecting and using photographs entirely. The complete cessation of Clearview's business is a devastating harm that far outweighs any speculative harm Plaintiffs have identified. And Plaintiffs have not offered to post a bond—which would need to be millions of dollars—to compensate Clearview for the period it would be wrongly put out of business while preliminary injunctive relief is in effect if Plainiffs do not prevail on the merits. Such a bond is required. Fed. R. Civ. P. 65(c).

Plaintiffs also seek to enjoin Clearview from "[c]ontinuing to possess, use and store" certain biometric data.[8] Br. at 2. The only way for Clearview to stop possessing and storing certain data would be to delete it. But Clearview is under a legal obligation to preserve data in connection with this lawsuit and other lawsuits. Ordering Clearview to destroy data that is being held for the purposes of complying with an obligation to preserve data would be prejudicial to Clearview, and could subject it to claims of spoliation and heavy sanctions. *See, e.g., S. New England Tel. Co. v. Glob. NAPs Inc.*, 624 F.3d 123, 147 (2d Cir. 2010) (affirming entry of default judgment against

[8] Clearview does not admit that it collects or stores information that is within the scope of BIPA. That is yet another defense that Plaintiffs have failed to address in their briefing.

defendants who intentionally deleted documents); *United States v. Philip Morris USA, Inc.*, 327 F. Supp. 2d 21, 26 (D.D.C. 2004) (imposing sanctions on defendant who spoliated evidence).

Finally, as noted above, an injunction would violate Clearview's First Amendment rights, which constitutes irreparable harm in itself. *Elrod v. Burns*, 427 U.S. 347, 373 (1976) ("The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury."); *ACLU v. Alvarez,* 679 F.3d 583, 589-90 (7th Cir. 2012) (even short deprivations of First Amendment rights constitute irreparable harm). The courts have recognized that it is in the public's interest not to enforce laws that violate the First Amendment. *Id.*

C. The Public Will Be Harmed If Clearview's Activities Are Enjoined

"In exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction." *Winter,* 555 U.S. at 24. "Sometimes an order granting or denying a preliminary injunction will have consequences beyond the immediate parties. If so, those interests . . . must be reckoned into the weighing process." *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 388 (7th Cir. 1984).

Plaintiffs assume the public interest is "the same as it is for Plaintiffs and class members." Br. at 15. To the contrary, an injunction could shut down Clearview's operations, which would hurt the public interest by preventing law enforcement from using Clearview's technology to identify victims and suspects in lawful criminal investigations.[9] *See* Metcalf Aff. ¶ 16 ("Clearview's technology helps protect children who would otherwise slip through the cracks—children who have not been reported as missing or abused and are being raped by their parents, family members, or others close to the child."); Webb Aff. ¶ 7 ("Put simply, the harm from sexual

[9] *See, e.g.*, Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. Times (Feb. 7, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

crimes committed against children can never be taken away. Clearview prevents these crimes from happening."); Williams Aff. ¶¶ 7-12 (detailing Clearview's role in rescuing a prepubescent child from "brutal sexual abuse" at the hand of her father, when all other investigative tools failed).

As described in the accompanying declarations, Clearview's app has been used for purposes vital to the public interest. If law enforcement could not use Clearview's app, it would impair their ability to solve crimes, including crimes of sexual exploitation targeting children. Metcalf Aff. ¶ 19 ("Without Clearview's facial recognition technology, hundreds of children would continue to be raped, and the recordings shared on the Internet for the world to see.").

IV. Plaintiffs Have Not Demonstrated That They Lack an Adequate Remedy at Law

To demonstrate that they lack an adequate remedy at law, Plaintiffs must show that traditional legal remedies, like money damages, are inadequate. *Roland Mach. Co.*, 749 F.2d at 386. Plaintiffs cannot satisfy this burden because BIPA provides an adequate remedy to Plaintiffs in the form of statutory damages. *See TD Bank N.A. v. Hill*, 928 F.3d 259, 282 (3d Cir. 2019).

CONCLUSION

Without offering any evidence, Plaintiffs are requesting the Court to enter a first-of-its-kind injunction that would likely put Clearview out of business, cause substantial harm to the public, and not prevent any harm to Plaintiffs. Plaintiffs' motion should be denied.

April 30, 2021

Respectfully submitted,

By: /s/ Lee Wolosky

Lee Wolosky (admitted pro hac vice)
Andrew J. Lichtman (pro hac vice pending)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022-3908
Phone: (212) 891-1600
lwolosky@jenner.com
alichtman@jenner.com

Howard S. Suskin
David P. Saunders
JENNER & BLOCK LLP
353 North Clark Street
Chicago, Illinois 60654
Phone: (312) 222-9350
hsuskin@jenner.com
dsaunders@jenner.com

Floyd Abrams (admitted pro hac vice)
Joel Kurtzberg (admitted pro hac vice)
CAHILL GORDON & REINDEL LLP
32 Old Slip
New York, NY 10005
Phone: (212) 701-3000
fabrams@cahill.com
jkurtzberg@cahill.com

Attorneys for Defendants Clearview AI, Inc., Hoan Ton-That, Richard Schwartz, Rocky Mountain Data Analytics LLC, and Thomas Mulcaire

CERTIFICATE OF SERVICE

I certify that on April 30, 2021 I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will then send a Notice of Electronic Filing to all counsel of record.

By: /s/ Lee Wolosky
Lee Wolosky